

This thesis focuses on the problem of the key size in McEliece cryptosystem and its solution using quasi-monoidic codes, especially quasi-monoidic Goppa codes. Required theory of quasi-monoidic Cauchy matrices and Goppa codes is introduced along with algebraic structures necessary for quasi-monoidic codes description. Suitable Abelian groups for this class of codes are specified. This thesis also presents efficient algorithms for constructing quasi-monoidic Cauchy matrices and quasi-monoidic Goppa codes. Reduction of the key size using this class of algebraic codes is presented as well.